DC3 Digital Forensics Challenge

101 - Detect Suspicious Software

Team Information

Team Name: Barely Legal

Results Email: [redacted]

Examination Time Frame: to 10/31/08

Instructions

Description: Locate any software title(s) as recorded in the provided registry files in the **101_Detect_Suspicious_Software_Challenge2008** folder that you suspect would be used in suspicious or illegal activities (other than standard OEM provided software or main named commercial products normally encountered). Report the exact registry key path, any additional entry information, the detailed explanation of your process (software or technique) used to examine and detect the information, and the reason you feel it could be used in suspicious or illegal activities.

Total Weighted Points: 20 Total Points available per entry – Total 100 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer: Points Awarded:

Date: Review Period: to

Completed: ☐ Yes ☐ No ☐ Partial

REPORT OF EXAMINATION

101 – Detect Suspicious Software

Item	Registry Key Path	Explanation
StegCreator Plus	SOFTWARE\NTRegistry\$$$PROTO.HIV\Microsoft\Windows\CurrentVersion\Uninstall\ StegCreatorPlus (E:\Program Files\StegCreatorPlus\iv_uninstall.exe)	Setganography program
Evidence Eliminator	HKEY_LOCAL_MACHINE\SOFTWARE\ EvidenceEliminator5.0	Program to delete user information from a hard disk .
Windows File Analyzer	NTUSER.DAT\NTRegistry\$$$PROTO.HIV\Software\MiTeC\WFA	A forensic analysis tool that decodes and analyzes some special files used by Windows OS.
Skype	NTUSER.DAT\NTRegistry\$$$PROTO.HIV\Software\Microsoft\Windows\CurrentVersion\ Explorer\MenuOrder\Start Menu\Programs\Skype	VOIP Software
USBDeview	NTUSER.DAT\NTRegistry\$$$PROTO.HIV\Software\Microsoft\Windows\CurrentVersion\ Explorer\UserAssist (G:\USB Forensics\USB Thumbview\USBDeview.exe)	utility that lists all USB devices connected to computer

METHODOLOGY / NOTES FORM

101 – Detect Suspicious Software

Date / Time	Notes
23-Oct-08 3:30 pm	Tool(s) Used: EnCase 6.11.2 by Guidance Software (www.encase.com) Windows Registry Recovery by MiTeC Software (http://www.mitec.cz/Downloads/WRR.zip) UserAssist.exe by Didier Stevens (http://didierstevens.com/files/software/UserAssist_V2_4_2.zip) Primary Investigation Created new case in EnCase. Imported all files in the "Registry Files" folder into EnCase as Single Files. Secondary investigation: Opened Software Registry file with Windows Registry Recovery (WRR). Viewed installed software by clicking "Windows Installation" icon and the "Installed Software" tab. Upon viewing notable software, I confirmed the findings in EnCase to get the actual Registry entry.